UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/721,504 | 11/26/2003 | Franck Le | 800.0186.U1(US) | 6168 |

29683 7590 06/11/2010

HARRINGTON & SMITH
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

| EXAMINER | |
|---|---|
| HENNING, MATTHEW T | |
| **ART UNIT** | **PAPER NUMBER** |
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/11/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/721,504 | LE ET AL. | |
| | Examiner | Art Unit | |
| | MATTHEW T. HENNING | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,4,11-15,18,42,43,50-56,59,60,63,64 and 66-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,11-15,18,42,43,50-56,59,60,63,64 and 66-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 3/12/2010.

## DETAILED ACTION

### *Response to Arguments*

Applicant's arguments filed 3/12/2010 have been fully considered but they are not persuasive.

Regarding the applicants' argument pertaining to the rejection of claims 66-68 under 35 USC 101, the examiner does not find the argument persuasive. While the amendment to the claims does limit the claims such that they no longer include a program *per se*, the scope of the claims now includes a transitory medium, which does not fall within one of the statutory categories of subject matter as explained below in the updated rejection of claims 66-68 under 35 USC 101.

Regarding the applicants argument that Gupta and Mitreuter do not teach that "the validity information further comprising public key information of a sending node comprising **an identity of an entity from which the public key of the sending node can be obtained**", the examiner does not find the argument persuasive.

First, the examiner notes that not all the claims now include this exact language. In fact, claims 63-67 now recite that the validity information comprises "an entity from which the public key of the sending node can be obtained". After examining the instant specification for guidance regarding this newly claimed limitation, the examiner found that "a database" is one example of an entity, and that "entity" had not been defined specifically by the applicants. A database is simply a structured file of records. As such, the examiner believes that the broadest reasonable interpretation of "an entity" can include "a file". Therefore, a certificate containing the public

key meets the limitation of "an entity from which the public key of the sending node can be obtained". Therefore, the examiner has maintained the rejection of claims 63-67 in view of Gupta and Mitreuter.

Further, it was well known for public key certificates to include "an identity" of itself, (it's certificate number for example), and as such would have been obvious to the ordinary person skilled in the art at the time of invention to have included the certificate number in the certificate. Therefore, the remainder of the independent claims remain obvious in view of Gupta and Mitreuter.

Further still, if the examiner were to interpret the limitation of "an identity of an entity from which the public key of the sending node can be obtained" more specifically to mean an entity outside of the packet or packet header, the claims would still remain obvious in view of Gupta, Mitreuter, and Yamagishi et al. (US Patent Number 7,136,998). Yamagishi teaches that in place of a public key certificate itself, a URL where the public key certificate has been put can be provided, in order to allow the latest public key certificate to be obtained.

All objections and rejections not set forth below have been withdrawn.

Claims *1,2,4,11-15,18,42,43,50-56,59,60,63-64 and 66-68* have been examined.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 66-68 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to a "computer readable storage medium comprising a computer program". In the event that such "computer readable storage media"

(hereinafter "media") are intended to be limited to the hardware and software necessary to transmit, transport, receive and process the computer program in such a manner as to enable the computer program to act as a computer component and realize its functionality, it is believed that the claims in question would be directed to patent-eligible subject matter (statutory). However, no such evidence that the embodiment covered by the claims in question which is directed to the "media" is limited to inclusion of such hardware and software elements exists. Therefore, it is believed that the "media" would reasonably be interpreted by one of ordinary skill as the abstract idea of any portion of a communication, including the forms of energy, *per se*, used in communications. Absent recitation of the hardware, the claims appear devoid of any physical articles or objects which may cooperate to achieve some function, and as such are not directed to a machine. Likewise, absent any such physical article or object, they cannot be directed to a manufacture. They are clearly not a series of steps or acts themselves, and as such are not a process. They are clearly not a composition of matter. Therefore, the claims in question do not appear to fall within a statutory category of invention as set forth in 35 USC 101.

***Claim Rejections - 35 USC § 103***

Claims 1-2, 15, 18, 42-43, 54-56, 59-60, and 63-64, and 66-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (US Patent Number 6,389,532) hereinafter referred to as Gupta, and further in view of Mitreuter et al. (US Patent Application Publication 20030033375) hereinafter referred to as Mitreuter.

Regarding claim 1, Gupta disclosed a method (See Gupta Fig. 1 Element 104, 108 or 112), comprising the steps of: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information

required to perform a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); the validity information comprising algorithm information to be used for performing the validity check of the packet and no pre-established security association is needed to verify the packet and algorithm initialization information(See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); generating a packet header (302), comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4) ; and sending the packet including the packet header from a first network node to a second network node (See Gupta Col. 6 Paragraph 4), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet. Furthermore, it was well know in the art at the time of invention for public key certificates to include therein information identifying the public key certificate, such as the certificate number. Therefore, it would have been obvious to the ordinary person skilled in the

art at the time of invention to have included the certificate number in the public key certificate. This would have been obvious because the ordinary person skilled in the art would have been motivated to utilize a conventional public key certificate.

Regarding claim 18, Gupta disclosed an apparatus comprising: validity information generating means for generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); packet header generating means for generating a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending means for sending the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2) and the validity information comprises algorithm information to be used for performing the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet. Furthermore, it was well know in the art at the time of invention for public key certificates to include therein information identifying the public key certificate, such as the certificate number. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included the certificate number in the public key certificate. This would have been obvious because the ordinary person skilled in the art would have been motivated to utilize a conventional public key certificate.

Regarding claim 42, Gupta disclosed an apparatus, comprising: a validity information generator configured to generate validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); a packet header generator configured to generate a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and a transmitter configured to send the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the

key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet. Furthermore, it was well know in the art at the time of invention for public key certificates to include therein information identifying the public key certificate, such as the certificate number. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included the certificate number in the public key certificate. This would have been obvious because the ordinary person skilled in the art would have been motivated to utilize a conventional public key certificate.

Regarding claim 55, Gupta disclosed an apparatus, comprising: a receiver configured to receive packets from a sending network node (See Gupta Fig. 1 Element 108, Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet and no pre-established security

association is needed to verify the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet. Furthermore, it was well know in the art at the time of invention for public key certificates to include therein information identifying the public key certificate, such as the certificate number. Therefore, it would have been obvious to the ordinary person skilled in the

art at the time of invention to have included the certificate number in the public key certificate. This would have been obvious because the ordinary person skilled in the art would have been motivated to utilize a conventional public key certificate.

Regarding claim 59, Gupta disclosed an apparatus, comprising: a transmitter configured to forward packets from a sending network node to a receiving network node (See Gupta Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet. Furthermore, it was well know in the art at the time of invention for public key certificates to include therein information identifying the public key certificate, such as the certificate number. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included the certificate number in the public key certificate. This would have been obvious because the ordinary person skilled in the art would have been motivated to utilize a conventional public key certificate.

Regarding claims 63 and 67, Gupta disclosed a method comprising: receiving packets (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); and performing a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of

a sending node comprising an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 64, Gupta disclosed a method comprising: forwarding received packets (Gupta Col. 7 Paragraph 2); and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (Gupta Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the

validity information further comprising public key information of a sending node comprising an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 66, Gupta disclosed a computer readable storage medium comprising a computer program (See Gupta Fig. 1 Element 104, 108 or 112), that when executed controls a processor to perform: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information required to perform a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); the validity information comprising algorithm information to be used for performing the validity check of the packet and no pre-established security association is needed to verify the packet and algorithm initialization information(See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); generating a packet header (302), comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4) ; and sending the packet including the packet header

from a first network node to a second network node (See Gupta Col. 6 Paragraph 4), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 68, Gupta disclosed a computer readable storage medium comprising a computer program (See Gupta Fig. 1 Element 104, 108 or 112), that when executed controls a processor to perform: forwarding received packets (Gupta Col. 7 Paragraph 2); and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (Gupta Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See

Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet. Furthermore, it was well know in the art at the time of invention for public key certificates to include therein information identifying the public key certificate, such as the certificate number. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included the certificate number in the public key certificate. This would have been obvious because the ordinary person skilled in the art would have been motivated to utilize a conventional public key certificate.

Regarding claims 2, 43, 56 and 60, Gupta and Mitreuter disclosed that the generating of the validity information comprises generating security information indicating security services applied to the packet (See Gupta Col. 5 Paragraph 7).

Regarding claim 15 and 54, Gupta and Mitreuter disclosed signing the packet using a private key corresponding to the public key indicated by the validity information in the packet header in a sending network node (See Gupta Col. 6 Paragraph 4 and Mitreuter Paragraph 0037).

Claims 4, 12-14, and 51-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta and Mitreuter as applied to claims 1 and 42 above, and further in view of Naudus (US Patent Number 6,202,081).

Regarding claims 12-14, and 51-53, Gupta and Mitreuter disclosed validation of packets, but failed to disclose that the step of generating the validity information comprises generating an information item for preventing replay attacks.

Naudus teaches that in a packet filtering system, packets should include timestamps in order to prevent replay attacks. Naudus further teaches that "[r]eplay attacks occur when a malicious user gains access to a router or other network device on a computer network that is forwarding data packets. Legitimate data packets are intercepted and then re-sent at a later time to allow the malicious user to appear as a legitimate user. A firewall helps prevent replay attacks by checking a time-stamp in the data packet that prevents the data packets from being re-sent at a later time." (See Naudus Col. 2 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Naudus in the packet validity checking system of Gupta and Mitreuter by including a timestamp in each packet and verifying the timestamp at the validity

checker. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent replay attacks in the network. In this combination, the inclusion of a timestamp in each packet, in itself, is an indication of a procedure to be used for anti replay attacks.

Regarding claim 4, Gupta and Mitreuter did not specifically teach that the step of generating the algorithm information comprises generating the algorithm information which indicates an algorithm to be used for performing the validity check of the packet. However, as taught by Naudus, in Col. 6 Line 60 - Col. 7 Line 7, it is well known to include in the packet header, an identification of which algorithm was used to sign the packet. As such, it would have been obvious to have included this information within the packet. Furthermore, the ordinary person skilled in the art at the time of invention would have recognized that this would allow for the user of a multiplicity of signature algorithms, as well as allowing updating of the signature algorithms in the future, and therefore it would have been obvious to have included an indication of the signature algorithm in the packet.

Claims 11, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta and Mitreuter as applied to claims 6 and 23 above, and further in view of Nikander (US Patent Number 7,155,500).

Gupta and Mitreuter disclosed including public key information within the packets, including the public key itself within the packets, but failed to specifically disclose that the step of generating the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the

sending node. Gupta did disclose that the public and private key pairs can be generated and stored in a certification server (See Col. 4 Paragraph 2).

Nikander teaches that by including the certificate of the public key, the receiving host can verify that the public key is truly owned by the sender (See Nikander Col. 10 Line 50 – Col. 12 Line 9).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Nikander in the packet verification system of Gupta and Mitreuter by including the public key certificate within each packet and verifying that the sender of each packet owned the public key used to sign the packet. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that a malicious node was not claiming to be a different node.

***Conclusion***

Claims *1,2,4,11-15,18,42,43,50-56,59,60,63-64 and 66-68* have been rejected.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571)272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Primary Examiner, Art Unit 2431